FIRST BASE technologies

TREND MICRO

# Smartwatch Security Research

# Overview

This report commissioned by Trend Micro in partnership with First Base Technologies reveals the security flaws of six popular smartwatches. The research involved stress testing these devices for physical protection, data connections and information stored to provide definitive results on which ones pose the biggest risk with regards to data loss and data theft.

# Summary of Findings

- Physical device protection is poor, with only the Apple Watch having a lockout facility based on a timeout. The Apple Watch is also the only device which allowed a wipe of the device after a set number of failed login attempts.
- All the smartwatches had local copies of data which could be accessed through the watch interface when taken out of range of the paired smartphone. If a watch were stolen, any data already synced to the watch would be accessible. The Apple Watch allowed access to more personal data than the Android or Pebble devices.
- All of the smartwatches we tested were using Bluetooth encryption and TLS over WiFi (for WiFi enabled devices), so consideration has obviously been given to the security of data in transit.
- Android phones can use 'trusted' Bluetooth devices (such as smartwatches) for authentication. This means that the smartphone will not lock if it is connected to a trusted smartwatch. Were the phone and watch stolen together, the thief would have full access to both devices.
- Currently smartwatches do not allow the same level of interaction as a smartphone; however it is only a matter of time before they do. Having unprotected devices with full access to personal data is a serious risk.

# Devices Tested

- Motorola 360 (Android Wear)
- LG G Watch (Android Wear)
- Sony Smartwatch 3 (Android Wear)
- Samsung Gear Live (Android Wear)
- Asus ZenWatch (Android Wear)
- Apple Watch (Watch OS)
- Pebble (Pebble OS)

# Timeline

Our research was conducted during July 2015.

# Background

- We examined the watches in their default state with no third party apps installed. Users should note that installing third party apps could increase the vulnerability of any smartwatch.
- We paired the watches with iPhone 5, Motorola X (2013) and Nexus 5.
- All watches were upgraded to the latest OS version at the time of testing (July 2015).

| Watch | OS version |
|---|---|
| Motorola 360 | Android OS 5.1.1<br>Android Wear 1.1.1.2006643 |
| LG G Watch | Android OS 5.1.1<br>Android Wear 1.1.1.1929530 |
| Sony Smartwatch | Android OS 5.1.1<br>Android Wear 1.1.1.1929530 |
| Samsung Gear Live | Android OS 5.1.1<br>Android Wear 1.1.1.1944630 |
| Asus ZenWatch | Android OS 5.1.1<br>Android Wear 1.1.1.1910765 |
| Apple Watch | Version 1.0.1 (12S632) |
| Pebble | Firmware v.2.9.1 |

# Device protection

- Authentication is not enabled by default on any device.
- Android phones (version 5.0 and above) can use 'trusted' Bluetooth devices such as smartwatches for authentication. This means that the phone will not engage the lock screen if it is connected to a trusted smartwatch. Were the phone and watch stolen together, the thief would have full access to both devices.


| Watch | Passcode | Type | Lockout |
|---|---|---|---|
| Motorola 360 | Not by default. Can be configured to turn on when the watch is taken off the wrist, but this did not work reliably during testing | Pattern | None, 1 minute timeout after 3 failed attempts. No timeout setting for automatic locking of the device. |
| LG G Watch | Not by default. | Pattern | None, 1 minute timeout after 3 failed attempts. No timeout setting for automatic locking of the device. |
| Sony Smartwatch | Not by default. Can be configured to turn on when the watch is taken off the wrist, but this did not work reliably during testing. | Pattern | None, 1 minute timeout after 3 failed attempts. No timeout setting for automatic locking of the device. |
| Samsung Gear Live | Not by default. | Pattern | None, 1 minute timeout after 3 failed attempts. No timeout setting for automatic locking of the device. |
| Asus ZenWatch | Not by default. | Pattern | None, 1 minute timeout after 3 failed attempts. No timeout setting for automatic locking of the device. |
| Apple Watch | Not by default. | 4 digit PIN (numbers only) | None by default, but can be configured to lock based on idle timeout. Option to erase data after 10 login attempts. |
| Pebble | Not available unless via third party apps. | - | - |

# Data Connections

- All the smartwatches support Bluetooth for data transmission between the watch and smartphone. These connections use Bluetooth encryption.
- Android and Pebble devices rely entirely on this encryption to secure the communication.
- The Apple Watch, as described in iOS Security Guide, integrates the proprietary IDS (Identity Services) technology as a further encryption layer.
- Four of the devices support using WiFi to keep the watch up-to-date when the paired phone is not in range.
- All of the connections over WiFi were encrypted using TLS 1.2 and it was not possible to intercept personal information.

| Watch | Bluetooth | WiFi |
|---|---|---|
| Motorola 360 | Yes | Yes |
| LG G Watch | Yes | No |
| Sony Smartwatch | Yes | Yes |
| Samsung Gear Live | Yes | Yes |
| Asus ZenWatch | Yes | No |
| Apple Watch | Yes | Yes |
| Pebble | Yes | No |

# Local data storage

- Local data storage was tested by turning off Bluetooth and Wi-Fi and checking what data was accessible from the watch interface.
- All the watches kept local copies of data available through the watch interface. If the watch were stolen any data already synced to the watch would be accessible.


| Watch | Cached data |
|---|---|
| Motorola 360 | Any unread notifications, historical fitness data, Google Keep entries, today's calendar entries. |
| LG G Watch | Any unread notifications, historical fitness data, Google Keep entries, today's calendar entries. |
| Sony Smartwatch | Any unread notifications, historical fitness data, Google Keep entries, today's calendar entries. |
| Samsung Gear Live | Any unread notifications, historical fitness data, Google Keep entries, today's calendar entries. |
| Asus ZenWatch | Any unread notifications, historical fitness data, Google Keep entries, today's calendar entries. |
| Apple Watch | Contacts, emails, calendars, pictures, fitness data and Passbook entries. The Passbook entries were tested with plane tickets. Passbook can also store loyalty cards with credit, so it should be possible to use this to make payments. |
| Pebble | Any unread notifications. Read notifications are also accessible via a notification history menu. This is also the only device that can be re-paired to a new phone without losing data. However, by default the device does not store any sensitive data (excluding notifications) unless via third party apps. |

## About First Base Technologies

Founded in 1989 by Peter Wood, First Base Technologies LLP provides independent security consultancy, testing and security awareness services. We pride ourselves on being ethical, pragmatic and professional, delivering quality services on time and within budget. The independence of our advice is guaranteed, since we have no commercial involvement in product sales or installation.

You will appreciate our commitment to maintaining a long-term business relationship, with expert opinion available on demand whenever you need it. Our CREST membership and our ISO 9001 and ISO 27001 certifications demonstrate a dedication to quality service and information security management that you can depend on. We don't just talk about information security, we live and breathe it.

Experts in their fields, our people are thought leaders in security counter-measures, analysis and emerging technologies. They work to the highest professional and ethical standards, whether they are providing advice, testing your defences or helping educate your staff. For over twenty-five years we have made significant contributions to the security of our clients and the environment in which they work. Major organisations in banking, insurance, fashion, retail, publishing, manufacturing, construction, law and government all trust our skills and results.

You can be sure that your information security is in safe hands.

## About the authors

### *Mike McLaughlin, Technical Team Lead, First Base Technologies LLP*

Mike is a Senior Penetration Tester and our Technical Team Lead. He is a talented and self-motivated ethical hacker working in the information security industry since 2006. For Mike, information security is a vocation not just a job - he is passionate about security whether in the corporate arena or personal home environment. He has worked on many security testing projects for clients in various business sectors, including retail, banking and government. Mike is a Member of the BCS and holds the SANS GSEC and GPEN qualifications. He was also the first member of our team to pass the demanding Offensive Security Certified Professional (OSCP) examination and is a CREST Registered Tester. Mike's key skills include a deep knowledge of network protocols and communications, operating systems and highly technical exploits.

### *Stefano Castilletti, Senior Penetration Tester, First Base Technologies LLP*

Stef is an enthusiastic Senior Penetration Tester with in-depth application testing skills. He brings coding and research skills to the team, as well as conducting complex web application and external infrastructure penetration tests. His training has also enabled him to perform custom tests requiring forensic and coding skills. Stef holds an MSc and a BSc (Hons) in Ethical Hacking and Computer Security from Abertay University, Dundee, is a Member of the BCS and holds the SANS GSEC and GWAPT qualifications. He has also achieved the Offensive Security Certified Professional (OSCP) certification and is a CREST Registered Tester. Stef's skills include exploiting both published and new vulnerabilities in applications, with particular focus on large e-commerce applications.

## About Trend Micro

Trend Micro Incorporated (TYO: 4704), a global leader in security software, strives to make the world safe for exchanging digital information. Our solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe.

For more information, visit www.trendmicro.co.uk Or
follow our news on Twitter at @TrendMicroUK.

Securing Your Journey to the Cloud